

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF WEST VIRGINIA**

IN THE MATTER OF THE SEARCH OF:

Messer Household
9957 Winchester Ave
Bunker Hill, West Virginia 25413

Case No. 3:19mj76

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, **Ellen Duffy**, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI), United States Department of Justice. As such, I am a law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7), and am empowered by law to conduct investigations and to make arrests for offenses enumerated in Title 18, United States Code Sections 2252, and 2252A.

2. I was hired by the FBI as a Special Agent in January 2018. I attended the FBI's training academy in Quantico, Virginia, where I received instruction regarding a variety of investigations, including investigations of crimes against children, drug trafficking, and violent gang offenses. I graduated from the FBI training academy as a Special Agent in May 2018. I am currently assigned to the Pittsburgh Division, sitting in Martinsburg, West Virginia, and I serve on the West Virginia Child Exploitation and Human Trafficking Task Force (WVCE&HTTF).

3. Prior to my employment with the FBI, I was employed with the University of Florida Police Department (UFPD) for approximately seven years. During my employment with UFPD, I served as a uniformed Patrol Officer, a Detective, and a Detective Sergeant. To qualify for this employment, I completed the Florida Department of Law Enforcement's Basic Field Training Course in October 2010. Prior to my employment with UFPD,

I was employed as a Special Agent with the United States Department of Education, Office of Inspector General for approximately two years. For that position, I completed the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in April 2008.

4. As part of my current duties as a Special Agent, I investigate criminal activity related to the possession, distribution and receipt of child pornography, in violation of Title 18, United States Code, Sections 2252 and 2252A. My experience includes, but is not limited to, reviewing examples of child pornography, conducting database checks, analyzing Internet Protocol (IP) address logs, reviewing forensic downloads of electronic devices, and writing affidavits for search warrants. I am familiar with matters including, but not limited to, means and methods used by possessors of child pornography to produce, transport, store, and distribute pornographic material.

5. Through my experience and training, I am aware that Title 18, United States Code, Section 2256 defines “minor,” for purposes of Section 2252, as “any person under the age of eighteen years.” Section 2256 also defines “sexually explicit conduct,” for purposes of Section 2252, as including: (a) genital-genital, oral-genital, anal-genital, and oral-anal sexual intercourse, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic; or (e) lascivious exhibition of the genitals or pubic area of any person.

6. This affidavit is submitted in support of an application for a search warrant authorizing a search of the residence and outbuildings located at 9957 Winchester Avenue, Bunker Hill, West Virginia, 25413, within the Northern District of West Virginia, hereinafter referred to as the “target premises” and further described in Attachment A, and incorporated herein by reference. From the target premises, I seek to seize evidence and instrumentalities of criminal violations that relate to the knowing possession, receipt, and distribution or attempted distribution

of child pornography. I request authority to search the entire target premises, including the residence and outbuildings for items specified in Attachment B, incorporated herein by reference, and to seize all items listed in Attachment B as evidence and instrumentalities of a crime.

7. In addition, based on my training and experience in related investigations and search warrants, and the experience of other law enforcement investigators I have communicated with, I am aware that it is common for items of digital media, including but not limited to laptop computers, flash drives, and cameras, to be transported or stored in motor vehicles. Therefore, I request that the search warrant authorize the search of any vehicles located at or near the target premises which fall under the dominion or control of the person or persons associated with the target premises.

8. I have obtained the information contained in this affidavit from my personal participation in the investigation and from reviewing information obtained through legal process, as well as from information obtained through law enforcement and commercial databases.

9. I have not included each and every fact known to me concerning the underlying investigation, as the sole purpose of this affidavit is to establish the required foundation for the requested search warrant. I have set forth only the facts that I believe are essential to establish this required foundation. Facts not set forth herein are not being relied upon in reaching my conclusion that an order should be issued. I do not request that this Court rely upon any facts not set forth herein in reviewing this affidavit and accompanying application.

10. Based on my training and experience and the facts set forth in this affidavit, there is probable cause to believe an unknown person(s) committed violations of 18 U.S.C. § 2252A(a)(2), which makes it a crime to receive and distribute material depicting the sexual exploitation of a minor, and 18 U.S.C. § 2252A(a)(4)(B), which makes it a crime to possess or

access with intent to view material depicting the sexual exploitation of a minor. As set forth herein, there is also probable cause to believe that evidence, fruits, and instrumentalities of these violations are located within the target premises identified in Attachment A.

PROBABLE CAUSE

11. On August 28, 2018, the National Center for Missing and Exploited Children (NCMEC) received CyberTipline Report 39363182 (hereinafter referred to as “the CyberTipline Report”) from Tumblr. Tumblr’s services include microblogging and social networking platforms that allow users to post multimedia and other content to Tumblr blogs. The CyberTipline Report identified 37 images depicting suspected child pornography uploaded to a Tumblr Account (hereinafter referred to as the “subject Tumblr account”) on August 28, 2018. The images were viewed by your affiant and your affiant confirmed that they contain child pornography.

12. The subject Tumblr account was created with electronic mail (“email”) address imhereforayoungtime@gmail.com; screen name “imhereforayoungtimee” and Uniform Resource Locator (URL) “imhereforayoungtimee.tumblr.com.”

13. The CyberTipLine Report also included a log of internet protocol (IP) addresses associated with posts made to the subject Tumblr account. Based on the information provided in the CyberTipline Report, the following steps were taken to identify the user of the subject Tumblr account:

a) *Administrative Subpoena 476073 Return from Tumblr*: On September 25, 2018, an administrative subpoena, along with a two-year non-disclosure order, was served to Tumblr to provide information pertaining to the subject Tumblr account. On November 8, 2018, Tumblr responded with the following information:

Blog: <https://imhereforayoungtimee.tumblr.com/>
 Account creation time: 2018-08-08 05:47:45
 User IP*: 2601:14a:8200:404:31f4:62bf:989c:185a
 Email Address: imhereforayoungtime@gmail.com

* Note: This is the most recent IP address from which the account or blog settings were saved.

b) *Administrative Subpoena 476072 Return from Google*: On September 25, 2018, an administrative subpoena, along with a two-year non-disclosure order, was served to Google to provide information pertaining to the Google account identified by the Google email address, imhereforayoungtime@gmail.com (hereinafter referred to as the “subject Google account”). On October 9, 2018, Google responded with the following subscriber information:

Name: YoDude

Email: imhereforayoungtime@gmail.com

Services: Gmail, Location History, Minutemaid, Web & App Activity

Created on: 2018/08/19-09:19:15-UTC

Terms of Service IP:

2600:1:f1b7:7b02:a930:6e09:5bf7:dbb0, on 2018/08/19-09:19:15-UTC

Google Account ID: 214484656886

Last Logins: 2018/08/31-07:10:45-UTC

Time	IP Address	Type
2018/08/31-08:53:24-UTC	2601:14a:8200:404:31f4:62bf:989c:185a	Login Comcast
2018/08/31-07:10:45-UTC	2601:14a:8200:404:31f4:62bf:989c:185a	Logout Comcast
2018/08/19-09:28:22-UTC	2601:14a:8200:404:2815:e0d9:6091:6657	Logout Comcast
2018/08/19-09:19:15-UTC	2600:1:f1b7:7b02:a930:6e09:5bf7:dbb0	Login Sprint

c) *Administrative Subpoenas 476070 and 495566 Returns from Comcast*: On September 25, 2018, and on January 3, 2019, administrative subpoenas were served to Comcast to provide information pertaining to two Tumblr login IP addresses from the log in

the CyberTipLine Report: 2601:14a:8200:404:88b7:c1c8:51de:5775 on 8/19/2018 at 14:35:58 EDT, and 2601:14a:8200:404:95dc:ae00:7ffc:126 on 2018-08-26 21:45:52 EDT. The responses from Comcast were received on October 9, 2018, and January 23, 2019, respectively. Both responses contained the following subscriber information:

Subscriber Name: Kimberly Messer

Service Address: 9957 Winchester Ave, Bunker Hill, WV 25413

Telephone #: (304) 995-6070

Account Number: 8299310030250993

Account Status: Active

IP Assignment: Dynamically Assigned

Email User Ids: messer9957; chiefs_mokinbul; Lemistry

d) Administrative Subpoena 503833 Return from Comcast: On February 7, 2019, an administrative subpoena was served to Comcast to provide information pertaining to Google login IP addresses 2601:14a:8200:404:2815:e0d9:6091:6657 on 2018/08/19-09:28:22-UTC, and 2601:14a:8200:404:31f4:62bf:989c:185a on 2018/08/31-07:10:45-UTC obtained from response to subpoena 476072. On February 7, 2019, Comcast responded with same subscriber information that it had provided in response to the preceding two subpoenas (subscriber Kimberly Messer of 9957 Winchester Ave, Bunker Hill, WV 25413).

14. As noted in paragraph 12 above, the email address of the subject Google account is linked to the subject Tumblr account in the Tumblr user's profile. Based on my training and experience, I am aware that Tumblr verifies a user's email address by sending a verification message to the email address. The Tumblr user must then take an action, such as providing a code from the verification message or following a hyperlink contained in the message, to verify that he

or she has access to the linked email account. Tumblr users update their email addresses by entering their current Tumblr password.

15. As noted in paragraph 13(b) above, in its response to administrative subpoena 476072, Google provided a total of three unique IP addresses that had accessed the subject Google account. Two of these IP addresses were recorded on the date the subject Google account was created, and the remaining IP address was recorded on the last date the subject Google account was accessed prior to the subpoena response being sent. All three of these IP addresses were also independently recorded by Tumblr as being associated with posts to the subject Tumblr account (as documented in the CyberTipLine report).

16. The following information was developed via open-source research and commercial databases: the target premises is associated with several individuals including Kimberly Messer, Tony Messer, Aaron Messer, and Chase Messer. K. Messer and T. Messer are married, and A. Messer and C. Messer are their sons. At the time of the suspect activity, A. Messer was 21 years of age and C. Messer was 19 years of age. As of June 13, 2019, the address listed on A. Messer's West Virginia driver's license was the target premises. No driver's license was located for C. Messer.

17. On June 13, 2019, I conducted surveillance at the target premises. I observed a red Ford F250 pickup truck with extensive body damage backed in against the south side of the house. I matched this vehicle to a truck in photographs on K. Messer's Facebook page. According to a post dated June 9, 2019, K. Messer and T. Messer were at a campground when the truck slid down a hill and struck another vehicle and a tree. T. Messer was also "tagged" in this post. The damage visible in the Facebook photographs matched damage I observed during surveillance.

18. In a post on K. Messer's Facebook page dated June 5, 2019, there was a photograph of lilies planted around a wooden sculpture. The post read, "My Lilly's are starting to bloom!" T. Messer was also "tagged" in this post. During surveillance on June 13, 2019, I observed the wooden sculpture, in the shape of a bear, surrounded by flowers in the front yard of the target premises.

19. In a post on K. Messer's Facebook page dated June 12, 2019, there were photographs of T. Messer standing in the front yard of the target premises.

BACKGROUND CONCERNING COMPUTERS AND CHILD PORNOGRAPHY

20. Based on my knowledge, training, and the experience and training of other law enforcement officers with whom I have had discussions, computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed. Computers basically serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

21. Child pornographers can transpose photographic images from a camera into a computer-readable format with the use of a scanner. With digital cameras, the images can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

22. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store thousands of images at very high resolution. The Internet affords collectors of child pornography several different venues for obtaining, viewing,

and trading child pornography in a relatively secure and anonymous fashion. Collectors and distributors of child pornography also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can often be found on the user's computer.

23. As with most digital technology, communications made from a computer are often saved or stored on that computer. Storing this information can be intentional, for example, by saving an e-mail as a file on the computer or saving the location of one's favorite websites in "bookmarked" files. Digital information can also be retained unintentionally. Traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or internet service provider client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces in a computer's web cache and Internet history files.

24. A forensic examiner often can recover evidence that shows whether a computer contains peer-to-peer software, when the computer was sharing files, and some of the files that were uploaded or downloaded. Computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a hard drive, deleted, or viewed via the Internet, using readily available forensic tools. Electronic files downloaded to a hard drive can be stored for years at little or no cost. When a person "deletes" a file on a home computer, the data

contained in the file does not actually disappear; rather, that data remains on the hard drive until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the hard drive that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or “cache.” The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user’s operating system, storage capacity, and computer habits.

**CHARACTERISTICS COMMON TO INDIVIDUALS INVOLVED IN RECEIVING
CHILD PORNOGRAPHY AND WHO HAVE A SEXUAL INTEREST IN CHILDREN
AND IMAGES OF CHILDREN**

25. Based on my previous investigative experience, and the training and experience related to child pornography investigations of other law enforcement officers with whom I have consulted, I have learned that individuals who produce, view, and receive multiple visual depictions of minors engaged in sexually explicit conduct are often individuals who have a sexual interest in children and in images of children, and that there are certain characteristics common to such individuals:

a. Such individuals commonly receive, distribute, and store child pornography electronically, by means including email, social media applications, blogs, and peer-

to-peer software. Such individuals commonly utilize false or fictitious online identities for the purpose of insulating themselves from detection from law enforcement.

b. Such individuals almost always possess and maintain their “hard copies” of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children typically retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica¹, and videotapes for many years.

c. Likewise, such individuals often maintain their collections that are in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These collections are often maintained for several years and are kept close by, usually at the collector’s residence, to enable the individual to view the collection that is valued highly.

d. Such individuals also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

¹ Child erotica, as used in this Affidavit and Attachments, is defined as items or depictions that may be sexually arousing to individuals with a sexual interest in children but which may not be obscene in and of themselves and do not necessarily depict minors engaged in sexually explicit conduct. Such materials may include non-sexually explicit photographs (such as minors depicted in undergarments in department store catalogs or advertising circulars), drawings, or sketches, written descriptions/stories, or journals.

e. Such individuals prefer not to be without their child pornography for any prolonged time period.

f. Such individuals commonly communicate by cellular phone or computer and often transmit their images from cellular phones to computers for storage. Such individuals commonly save their communications, images and videos of child exploitation material to their cellular phones, computers, thumb drives and other electronic storage media.

g. Based on my previous training and investigative experience, and the training and experience related to child pornography investigations of other law enforcement officers with whom I have consulted, I am also aware that individuals who have a sexual interest in children and in images of children sometimes encounter a minor on the Internet and induce or coerce the minor to produce a visual depiction of the minor engaged in sexually explicit conduct. Communications related to such inducement or coercion may occur through online communication channels such as online chats or emails. I am aware that computers and other electronic devices that have been used for such communications may contain evidence of those communications.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

26. Searches and seizures of evidence from computers commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following reasons:

1. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magnetic opticals, and others) can store the equivalent of millions of pages of information. Especially when the user wants to conceal criminal evidence, he or

she often stores it in random order with deceptive filenames. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

2. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

27. In order to fully retrieve data from a computer system, the analyst must access all magnetic storage devices as well as the central processing unit ("CPU"). In cases involving child pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient examination due to various software and hardware configurations. In addition, the analyst must also examine the system software (operating systems or interfaces, and hardware drives) and any applications software which may have been used to create the data (whether stored on hard drives or on external media).


28. Furthermore, because there is probable cause to believe that the computer and its storage devices are all instrumentalities of crimes within the meaning of 18 U.S.C. §§ 2251 through 2256, they should all be seized as such.

CONCLUSION

29. Based upon the information contained in this application and affidavit, there is probable cause to conclude that at the target premises there exists evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252, and 2252A, which makes it a crime to possess, receive and distribute material depicting the sexual exploitation of a minor. Your affiant, therefore, respectfully requests that the attached warrant be issued authorizing the search of the target premises described in Attachment A, for the items listed in Attachment B.

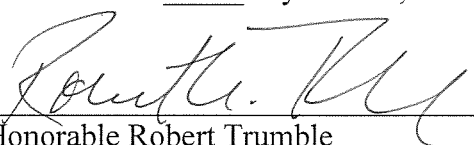
The information in this affidavit is true to the best of my knowledge and belief.

FURTHER AFFIANT SAYETH NAUGHT



Ellen D. Duffy
Special Agent, FBI

Subscribed and sworn to before me this 20th day of June, 2019.



Honorable Robert Trumble
United States Magistrate Judge
Northern District of West Virginia